AMENDED IN SENATE JUNE 15, 2015

AMENDED IN ASSEMBLY APRIL 6, 2015

CALIFORNIA LEGISLATURE—2015–16 REGULAR SESSION

ASSEMBLY BILL No. 670

Introduced by Assembly Member Irwin

February 25, 2015

An act to amend Section 11549.3 of the Government Code, relating to technology.

LEGISLATIVE COUNSEL'S DIGEST

AB 670, as amended, Irwin. ~~Security assessments.~~ *Information technology security.*

~~Existing~~

(1) Existing law ~~establishes~~ *establishes, within the Government Operations Agency,* the Department of Technology ~~within the Government Operations Agency, headed by~~ *under the supervision of* the Director of ~~Technology~~ *Technology,* who is also known as the State Chief Information Officer. The department is *generally* responsible for the approval and oversight of information technology projects by, among other things, consulting with *state* agencies during initial project planning to ensure that project proposals are based on well-defined programmatic needs.

Existing law ~~establishes~~ *establishes, within the department,* the Office of ~~Technology Services within the department,~~ *Information Security* under the supervision of the Chief of the Office of ~~Technology Services, and~~ *Information Security. Existing law* sets forth ~~its duties,~~ *the authority of the office,* including, but not limited to, the authority to ~~conduct~~ *conduct,* or require ~~a~~ *to be conducted, an independent* security

assessment of any state agency, ~~as prescribed.~~ *department, or office the cost of which is to be funded by the state agency, department, or office being assessed.*

This bill would, instead, *impose a duty on the office to* require ~~the office~~ *it* to conduct, or ~~require, an~~ *require to be conducted, an independent security* assessment of every state ~~agency~~ *agency, department, or office* at least once every 2 years and would ~~require~~ *maintain the requirement that* the state ~~agency~~ *agency, department, or office* being ~~audited to pay~~ *assessed fund* the costs of the *independent* security assessment. ~~The~~ *This* bill would *require an independent security assessment to include specific components, to the extent possible, and* authorize the department to require ~~agencies that are~~ *a state agency, department, or office* not in compliance *with any recommendation made in the independent security assessment* to redirect *its* available ~~funding~~ *and authorized funds* to pay the costs of ~~the assessments. The bill would require the department to adopt standards, to be included within the State Administrative Manual, setting forth the manner for the assessed agency to communicate the assessment results to the department.~~ *complying with the recommendation.*

~~This bill would authorize the Governor's Office of Emergency Services to conduct the strategic direction of security assessments performed by the Military Department's Computer Network Defense Team, and would require those assessments to contain certain elements.~~

This bill would require the results of an independent security assessment to be available only to the state agency, department, or office that was assessed. This bill would restrict the transmission or communication of the results of an independent security assessment and any related information to state government employees and state contractors who have been approved as necessary to receive this information in order to perform the assessment. The bill would require the department to adopt standards, to be included within the State Administrative Manual, setting forth the manner for the aggregate of the results of an independent security assessment to be transmitted to the department.

This bill would deem the results of an independent security assessment, the aggregate of the results of an independent security assessment transmitted to the department, and any related information as confidential and prohibit their disclosure pursuant to any state law, including, but not limited to, the California Public Records Act. This bill would require data produced during the creation of an independent

security assessment to be destroyed within 1 year of its date of creation, unless the Office of Emergency Services determines that retention for a longer period of time is necessary for state security.

This bill would also authorize the Military Department to perform an independent security assessment as described above. This bill would authorize the Military Department to mitigate the impact of a cyber attack or assist a law enforcement investigation into cyber security upon the request of the Office of Emergency Services, a state law enforcement agency, or a state agency, department, or office. This bill would further authorize the Military Department to perform a cyber security assessment or respond to a cyber security incident impacting state infrastructure upon the request of the Office of Emergency Services.

~~Existing~~

(2) Existing law requires that a statute that limits the public's right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings to demonstrate the interest protected by the limitation and the need for protecting that interest.

This bill would limit access to *the results of an independent* security assessment ~~results,~~ *and related records* and would make findings to demonstrate the interest protected by the limitation and the need for protecting that interest.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 11549.3 of the Government Code is amended to read:

11549.3. (a) The director shall establish an information security program. *The office shall report to the Department of Technology any state agency found to be noncompliant with information security program requirements.* The program responsibilities include, but are not limited to, all of the following:

(1) The creation, updating, and publishing of information security and privacy policies, standards, and procedures for state agencies in the State Administrative Manual.

(2) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies to effectively manage security and risk for both of the following:

(A) Information technology, which includes, but is not limited to, all electronic technology systems and services, automated information handling, system design and analysis, conversion of data, computer programming, information storage and retrieval, telecommunications, requisite system controls, simulation, electronic commerce, and all related interactions between people and machines.

(B) Information that is identified as mission critical, confidential, sensitive, or personal, as defined and published by the Office of Information Security.

(3) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies for the collection, tracking, and reporting of information regarding security and privacy incidents.

(4) The creation, issuance, and maintenance of policies, standards, and procedures directing state agencies in the development, maintenance, testing, and filing of each agency's disaster recovery plan.

(5) Coordination of the activities of agency information security officers, for purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards.

(6) Promotion and enhancement of the state agencies' risk management and privacy programs through education, awareness, collaboration, and consultation.

(7) Representing the state before the federal government, other state agencies, local government entities, and private industry on issues that have statewide impact on information security and privacy.

(b) An information security officer appointed pursuant to Section 11546.1 shall implement the policies and procedures issued by the Office of Information Security, including, but not limited to, performing both of the following duties:

(1) Comply with the information security and privacy policies, standards, and procedures issued pursuant to this chapter by the Office of Information Security.

(2) Comply with filing requirements and incident notification by providing timely information and reports as required by policy or directives of the office.

(c) *(1)* The office shall conduct, or require to be conducted, an independent security assessment of every state agency, department, or office at least once every two years. The cost of the *independent* security assessment shall be funded by the state agency, department, or office being assessed. ~~The assessment results shall be made available only to the assessed entity.~~ The *independent security* assessment shall include, to the extent practicable, all of the following ~~components, which~~ *components and* shall be conducted in compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Controls:

~~(1)~~

(A) Vulnerability scanning, that includes, but is not limited to, all of the following:

~~(A)~~

(i) Validation that IT systems have currently supported software, with all necessary security patches and updates applied.

~~(B)~~

(ii) Validation that system security configurations are in compliance with NIST standards.

~~(C)~~

(iii) Validation that the network architecture is arranged so as to separate internal, publicly accessible, and external zones, along with a mechanism to identify and alert on attempted intrusions.

~~(2)~~

(B) Penetration testing, when determined appropriate by the ~~Governor's~~ Offices of Emergency Services.

~~(3)~~

(C) A report on the number, severity, and nature of identified vulnerabilities and recommendations for remediation and risk mitigation.

(2) (A) The Military Department may perform an independent security assessment required by paragraph (1).

(B) The Military Department may mitigate the impact of a cyber attack or assist a law enforcement investigation into cyber security upon the request of the Office of Emergency Services, a state law enforcement agency, or a state agency, department, or office.

(C) The Miliary Department may perform a cyber security assessment or respond to a cyber security incident impacting state infrastructure upon the request of the Office of Emergency Services.

~~(d) The office shall report to the Department of Technology any state agency found to be noncompliant with information security program requirements.~~

~~(e)~~

(d) The Department of Technology may require ~~that any agency in noncompliance with subdivision (c)~~ *a state agency, department, or office to* redirect any funds within ~~the agency's budget,~~ *its budget* that may be legally expended for these purposes, ~~for the purposes of paying~~ *to pay* the costs of ~~compliance~~ *becoming compliant* with ~~subdivision (c).~~ *any recommendation made in an independent security assessment.*

~~(f) The Governor's Office of Emergency Services may conduct the strategic direction of security assessments performed by the Military Department's Computer Network Defense Team, as budgeted in Item 8940-001-0001 of the Budget Act of 2014. Each assessment shall include all of the following:~~

~~(1) Contracting and negotiations with state agencies, departments, and offices, or private entities to be assessed.~~

~~(2) Setting an assessment calendar to be followed by the CND–T.~~

~~(3) Prioritizing of incident response.~~

(e) (1) The office, Military Department, or entity required to conduct an independent security assessment pursuant to subdivision (c) shall transmit the results of that assessment only to the state agency, department, or office that was the subject of that assessment.

(2) The office, Military Department, or entity required to conduct an independent security assessment pursuant to subdivision (c) shall transmit an aggregate of the results of that assessment to the Department of Technology.

~~(g)~~

(3) The Department of Technology shall adopt standards, to be included within the State Administrative Manual, setting forth the ~~manner~~ *requirements* for the ~~assessed agency to communicate the~~ *office, Military Department, or entity required to conduct an independent security assessment pursuant to subdivision (c) to transmit, pursuant to paragraph (2), the aggregate of the results*

of that assessment ~~results~~ to the ~~department,~~ *Department of Technology,* including, but not limited to, all of the following:

~~(1)~~

(A) Aggregated, statistical information relevant to the assessment results, including, but not limited to, the number of identified vulnerabilities categorized by high, medium, and low risk. These results shall not include any specific information relative to the nature of the risk that is potentially exploitable.

~~(2)~~

(B) Prioritization of vulnerabilities.

~~(3)~~

(C) Identification of relevant internal resources.

~~(4)~~

(D) Strategy for addressing and mitigating those vulnerabilities.

~~(h) Communication of assessment results shall be restricted to only approved government employees and validated contractors. Assessment results and related aggregated reports shall be confidential and, pursuant to Section 6254.19, shall be exempt from disclosure under the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1).~~

~~(i) Data produced by assessments shall be retained by all parties for no longer than one year, unless the Governor's Office of Emergency Services determines that retention for a longer period is necessary.~~

(f) (1) Transmission or communication of the results of an independent security assessment performed pursuant to subdivision (c) and any related information shall be restricted to state government employees and state contractors who have been approved as necessary to receive this information in order to perform that assessment by the office, Military Department, or entity required to conduct the independent security assessment.

(2) The results of an independent security assessment performed pursuant to subdivision (c), the aggregate of the results of an independent security assessment transmitted to the Department of Technology pursuant to subdivision (e), and any related information are confidential and shall not be disclosed pursuant to any state law, including, but not limited to, the California Public Records Act (Chapter 3.5 (commencing with Section 6250) of Division 7 of Title 1).

(3) Data produced during the creation of an independent security assessment performed pursuant to subdivision (c) shall be destroyed within one year of its date of creation, unless the Office of Emergency Services determines that retention for a longer period of time is necessary for state security.

SEC. 2. The Legislature finds and declares that Section 1 of this act, which amends Section 11549.3 of the Government Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

The state has a very strong interest in protecting its information technology systems from intrusion, because those systems *contain confidential information and* play a critical role in ~~assisting the entities~~ *the performance of the duties* of state ~~government in carrying out their duties.~~ *government.* Thus, information regarding the specific vulnerabilities of those systems ~~should be~~ *must be* protected ~~at least until those vulnerabilities have been remediated so as~~ to preclude use of that information to facilitate attacks on those systems.

O